

REMARKS

Claims 1-61 are in the application. Claims 1-61 were rejected.

Applicants respectfully respond to this Office Action.

Claim Rejections under 35 U.S.C. § 102

Claims 1-6, 12-16, 22-27, 31-35, 41-46, and 52-56 were rejected under 35 U.S.C. § 102(b) as being anticipated by European Patent No. 1 001 570 A2 to Berenzweig et al. (hereinafter “Berenzweig”).

“A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.” M.P.E.P. § 2131 (Aug. 2001) (*quoting Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)). “The identical invention must be shown in as complete detail as is contained in the . . . claim.” *Id.* (*quoting Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1051, 1053 (Fed. Cir. 1987)). In addition, “the reference must be enabling and describe the applicant’s invention sufficiently to have placed it in possession of a person of ordinary skill in the field of the invention.” *In re Paulsen*, 30 F.3d 1475, 1479, 31 USPQ2d 1671, 1673 (Fed. Cir. 1994)

Applicants respectfully submit that claims 1-6, 12-16, 22-27, 31-35, 41-46, and 52-56 are not anticipated by Berenzweig for the reasons and explanations set forth below.

With respect to claim 1, Applicants respectfully submit that Berenzweig does not disclose all of the limitations of claim 1. In particular, Berenzweig does not disclose “generating a radio access network key (RAK) as a function of the random number and a key selected from the group consisting of a public land mobile network key (PK) and a broadcast access key (BAK); and generating a temporary registration key (RGK) as a function of the RAK.”

Berenzweig discloses efficient authentication with key update. (Title) The method for performing authentication is provided by using an authentication challenge transmitted to a terminal to provide the terminal with the information to calculate authentication and cipher key values. (Abstract) A single random value is transmitted to a mobile or stationary terminal. This

single random value is used to both update the authentication and cipher key values of the terminal and also to provide an authentication challenge to the terminal. (Col. 5, lines 25-29) A visiting authentication center obtains a random value R_T , an authentication key value K_A and a cipher key value K_C from a home authentication center. The visiting authentication center then transmits the random number R_T to the terminal to update the terminal's authentication key and cipher key values, and to challenge the terminal as part of an authentication process. (Abstract) The terminal uses R_T to calculate authentication key value K_C , and to respond to the visiting authentication center's challenge. (Abstract)

The Examiner cites Berenzweig as disclosing "generating a radio access network key (RAK) $\{K_A = F^A(R_T, K_i)\}$ as a function of the random number and a key selected from the group consisting of a public land mobile network key (PK) $\{K_i\}$ and a broadcast access key (BAK)" and cites Col. 5, lines 30-57. The cited portion reads as follows:

Mobile or stationary terminal 70, and home location register 72 share key value K_i . When mobile terminal 70 requests access to a visiting network, the visiting authentication center contacts the home authentication center to obtain the random value R_T , the authentication key value K_A and cipher key value K_C . In response to this request, the home authentication center accesses the home location register 72 associated with mobile terminal 70 using an identifier such as a telephone number provided by the mobile terminal via the visiting authentication center. The home authentication center then calculates authentication key value K_A by taking the output of cryptographic function F^A using random number R_T as an input and the value K_i as a key input. Additionally, the home authentication center calculates the cipher key value K_C using the output of cryptographic function F^C using the value R_T as an input and the value K_i as a key input. Once these values calculated, the home authentication center communicates the values R_T , K_A , and K_C to the visiting authentication center. The visiting authentication center then stores the values K_A , K_C , and R_T in the visiting location register associated with mobile terminal 70. The visiting authentication center then communicates the value R_T to mobile terminal 70 as both an authentication challenge and as a value that will be used to update the authentication and cipher key values used by the mobile terminal.

Berenzweig is silent concerning a broadcast access key. In addition, nothing is suggested regarding selecting a key from a group that includes a broadcast key. Berenzweig deals with the situation of a traveling mobile terminal that must be re-authenticated before it is allowed access. Therefore, because Berenzweig does not disclose this limitation, Applicants respectfully request that the rejection of claim 1 be withdrawn.

In addition, Berenzweig does not disclose “generating a temporary registration key (RGK) as a function of the RAK.” The Examiner cites Col. 5, lines 43-46 as disclosing this limitation. After reviewing the above cited portion of the Berenzweig reference, which includes the cited lines, Applicants are unable to find any disclosure of “generating a temporary registration key (RGK) as a function of the RAK.” The cited portion discloses calculating the cipher key value, with no indication that this is a “temporary registration key.”

Applicants respectfully request that the rejections of claims 1, 12, 22, 31, 35, 41, and 52 be withdrawn as the Berenzweig reference does not disclose all the limitations of these claims. Applicants further submit that claims 13, 32, and 53 are allowable as depending directly from an allowable base claim.

Claims 2, 23, and 42 are allowable as depending directly from an allowable base claim.

Claims 3, 14, 24, 33, and 43 are allowable as depending directly or indirectly from an allowable base claim. These claims are also allowable for the following reasons. The Examiner states that Berenzweig discloses “further comprising receiving a provisioning message from a broadcast-multicast service center” and cites Col. 6, lines 25-30. The cited portion reads as follows:

...value R_M as an input and the value K_A as a key input. This output value is then communicated to the mobile terminal where the terminal independently determines the output function F^2 with the value R_M as an input and the value K_A as a key input. If the output values match, the mobile terminal then verifies or authenticates the visiting network.

Berenzweig is silent regarding “a provisioning message from a broadcast-multicast service center.” The cited portion is part of the challenge-authentication process of the Berenzweig method. Applicants respectfully submit that claim limitation “further comprising receiving a

provisioning message from a broadcast-multicast service center” are not disclosed by the Berenzweig reference and request that the rejections be withdrawn.

Claims 4, 15, 25, 34, 44, and 55 are allowable for the same reasons given above for claims 3, 14, 24, 33, and 43.

Claims 5, 25, 26, 45, and 54 are allowable for the same reasons given above for claims 3, 14, 24, 33, and 43.

Claims 6, 16, 27, 35, 46, and 56 are allowable as depending either directly or indirectly from an allowable base claim.

Claim Rejections under 35 U.S.C. § 103

Claims 7, 17, 28, 36, 47, and 57 were rejected as being unpatentable over Berenzweig in view of U.S. Patent 7,114,175 to Lahtenmaki (hereinafter “Lahtenmaki”). This rejection is respectfully traversed.

To establish a prima facie case of obviousness, the prior art reference (or references when combined) must teach or suggest all the claim limitations. “The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in Applicants’ disclosure.” In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

Applicants submit that the nonobviousness of independent claims 1, 12, 22, 31, 41, and 52 precludes a rejection of claims 7, 17, 28, 36, 47, and 57 depending therefrom, because a dependent claim is obvious only if the independent claim from which it depends is also obvious. See In re Fine, 5, U.S.P.Q. 2d 1595, 1600 (Fed. Cir. 1988), *see also* MPEP § 2143.03. Therefore, the Applicants request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejections to dependent claims 7, 17, 28, 36, 47, and 57.

Claims 8, 9, 18, 19, 37, 38, 48, 49, 58, and 59 were rejected as being unpatentable over Berenzweig in view of U.S. Patent Publication No. 20040022216A1 to Shi (hereinafter “Shi”). This rejection is respectfully traversed.

To establish a prima facie case of obviousness, the prior art reference (or references when combined) must teach or suggest all the claim limitations. “The teaching or suggestion to make

the claimed combination and the reasonable expectation of success must both be found in the prior art, not in Applicants' disclosure." In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

Applicants submit that the nonobviousness of independent claims 1, 12, 22, 31, 41, and 52 precludes a rejection of claims 8, 9, 18, 19, 37, 38, 48, 49, 58, and 59 depending therefrom, because a dependent claim is obvious only if the independent claim from which it depends is also obvious. See In re Fine, 5, U.S.P.Q. 2d 1595, 1600 (Fed. Cir. 1988), see also MPEP § 2143.03. Therefore, the Applicants request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejections to dependent claims 8, 9, 18, 19, 37, 38, 48, 49, 58, and 59.

Claims 10, 11, 20, 21, 29, 30, 39, 40, 50, 51, 60, and 61 were rejected as being unpatentable over Berenzweig in view of U.S. Patent 5,371,794 to Diffie et al. (hereinafter "Diffie"). This rejection is respectfully traversed.

To establish a prima facie case of obviousness, the prior art reference (or references when combined) must teach or suggest all the claim limitations. "The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in Applicants' disclosure." In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

Applicants submit that the nonobviousness of independent claims 1, 12, 22, 31, 41, and 52 precludes a rejection of claims 10, 11, 20, 21, 29, 30, 39, 40, 50, 51, 60, and 61 depending therefrom, because a dependent claim is obvious only if the independent claim from which it depends is also obvious. See In re Fine, 5, U.S.P.Q. 2d 1595, 1600 (Fed. Cir. 1988), see also MPEP § 2143.03. Therefore, the Applicants request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejections to dependent claims 10, 11, 20, 21, 29, 30, 39, 40, 50, 51, 60, and 61.

REQUEST FOR ALLOWANCE

In view of the foregoing, Applicants submit that all pending claims in the application are patentable. Accordingly, reconsideration and allowance of this application are earnestly solicited. Should any issues remain unresolved, the Examiner is encouraged to telephone the undersigned at the number provided below.

Respectfully submitted,

Dated: May 10, 2007

By: /Roberta A. Young/
Roberta Young, Reg. No. 53,818
(858) 658-5803

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 658-5787
Facsimile: (858) 658-2502